Institutional Repository - Research Portal
Dépôt Institutionnel - Portail de la Recherche
researchportal.unamur.be
University of Namur

RESEARCH OUTPUTS / RÉSULTATS DE RECHERCHE

Les responsabilités liées à la diffusion d'informations illicites et inexactes sur Internet

Montero, Etienne

Published in:
Internet face au droit

Publication date:
1997

Document Version
le PDF de l'éditeur

Link to publication

Citation for pulished version (HARVARD):
Montero, E 1997, Les responsabilités liées à la diffusion d'informations illicites et inexactes sur Internet. Dans *Internet face au droit.* Cahiers du CRID, Numéro 12, Story Scientia, Bruxelles, p. 111-137.

General rights
Copyright and moral rights for the publications made accessible in the public portal are retained by the authors and/or other copyright owners and it is a condition of accessing publications that users recognise and abide by the legal requirements associated with these rights.

- Users may download and print one copy of any publication from the public portal for the purpose of private study or research.
- You may not further distribute the material or use it for any profit-making activity or commercial gain
- You may freely distribute the URL identifying the publication in the public portal ?

Take down policy
If you believe that this document breaches copyright please contact us providing details, and we will remove access to the work immediately and investigate your claim.

Download date: 05. May. 2023

Chapitre 4 - Les responsabilités liées à la diffusion d'informations illicites ou inexactes sur Internet

par Etienne MONTERO*

* Chargé de cours, F.U.N.D.P.

I. Introduction

1. Manifestement, Internet fascine les uns autant qu'il suscite inquiétude et émotion chez les autres... et laisse, en définitive, peu de monde indifférent. Bercés par l'illusion d'un espace de liberté totale et sans bornes, les premiers ont tendance à crier à la censure, si d'aucuns s'avisent de rappeler que des règles existent et qu'Internet n'y échappe pas. Les autres, au contraire, en appellent à des mesures de contrôle voire à la censure préalable et sont tentés de réclamer l'adoption de réglementations spécifiques et contraignantes.

Ainsi, dans les deux camps, il est des profanes, mais aussi certains juristes (ce qui est plus troublant...), pour penser que le droit ne s'y retrouve plus face à Internet, ce qui les satisfait ou les désole, c'est selon.

Des deux côtés, l'erreur procède de la même racine : une méconnaissance de ce qu'est au juste Internet et la propension, un peu naïve, à le considérer comme un « espace virtuel », étranger au « monde réel ». Tout se passe comme si le droit de ce monde était inapte à régir les actes délictueux commis dans le nouveau « monde virtuel ».

Il est dans notre intention de montrer la fausseté de pareille perception, sans vouloir nier pour autant certaines difficultés inhérentes à la mise en oeuvre des responsabilités. Difficultés, faut-il le dire, qui ne sont pas nécessairement propres à Internet, tant il est vrai qu'on s'y heurte aussi, au quotidien, pour le règlement de litiges très terre à terre. En réalité, ces difficultés tiennent, pour la plupart, à la complexité du droit tout simplement[320].

Objet, limites et plan de l'exposé

2. De façon schématique, on peut admettre qu'il existe actuellement trois modes de diffusion de l'information sur Internet : le courrier électronique (« E-mail »), les forums de discussion (ou « newsgroups ») et les serveurs d'information (dont le plus utilisé est aujourd'hui le « Web », un système d'informations distribuées auquel on peut accéder en mode « hypertexte »)[321].

Le courrier électronique est un service permettant l'échange de messages exclusivement destinés à une ou plusieurs personnes, physiques ou morales, déterminées et individualisées. A ce titre, on considère généralement qu'il relève du secret de la correspondance privée. Or, l'affirmation

320 En ce sens, voy. déjà M. VIVANT, « Cybermonde : Droit et droits des réseaux », *J. C. P.*, G, 1996, I, 3969, *passim*.

321 Pour une présentation générale des services disponibles sur Internet, voy. G. BASQUE, « Introduction à l'Internet », 15 p., disponible sur Internet (http://www.droit.umontreal.ca/ CRDP); A. DUFOUR, *Internet*, Coll. Que sais-je?, Paris, P. U. F., 2e éd., 1996, 127 p.; B. LIPS, *Internet en Belgique*, Bruxelles, Best Of Editions, 1996, spéc. le chapitre 3.

du droit au respect de la vie privée s'oppose aux intrusions et aux pratiques de surveillance ou de contrôle. On ne saurait donc tenir pour responsables les intermédiaires techniques (transporteurs, gestionnaires de réseau, fournisseurs d'accès et serveurs) en raison des éventuels dommages occasionnés dans le contexte du courrier électronique. Logiquement, la responsabilité pèse sur le seul auteur des messages litigieux. On notera toutefois que certains maîtres de réseaux locaux s'autorisent à fouiller le courrier électronique des personnes placées sous leur responsabilité. Dans ce cas, ils s'exposent à un standard plus élevé de responsabilité.

On s'attachera surtout à déterminer les responsabilités liées aux informations diffusées dans le cadre des groupes de discussion et par le biais des multiples serveurs localisés aux quatre coins du globe.

3. Le contentieux relatif à la diffusion d'informations inexactes ou illicites est particulièrement diversifié. Dans certains cas, la victime est le destinataire d'informations non conformes (inexactes, périmées...) à son attente légitime ou non désirées. D'autres fois, il peut s'agir d'un tiers, éventuellement non utilisateur du réseau, visé ou concerné par une information diffamatoire, tendancieuse... Encore que la malice humaine s'exprime dans des formes dont la variété est presque infinie. Ainsi, doivent être tenues pour illicites les informations communiquées au mépris des règles relatives à l'intégrité du processus judiciaire (respect du secret de l'instruction...); celles qui portent atteinte à l'honneur, à la bonne réputation (calomnie, diffamation...), au respect de la vie privée, au droit à l'image; celles transmises en violation des lois particulières interdisant la diffusion de certains types d'informations (à caractère raciste ou antisémite, propagande haineuse, incitation à la violence...); celles qui sont contraires à l'ordre public (outrage à magistrat, au chef de l'Etat...) ou aux bonnes moeurs (obscénité, harcèlement...); les informations attentatoires à la protection des mineurs (pédophilie...); celles qui constituent des contrefaçons d'oeuvres protégées par le droit d'auteur, etc.

On aperçoit aisément la diversité des questions soulevées ainsi que des règles de droit et des sanctions susceptibles de jouer. Il est entendu que notre approche se situe à un niveau de généralité qui ne permet pas de descendre dans le détail de chacun des dispositifs légaux ou réglementaires applicables. Par ailleurs, le droit pénal spécial ne sera pas abordé, d'autant qu'il fait l'objet d'une contribution distincte[322]. Malgré leur intérêt, diverses techniques juridiques permettant de rétablir la vérité ou de mettre fin à l'atteinte portée à un intérêt devront également être passées sous silence. On songe : au *droit de réponse*, que le gestionnaire d'une page Web ou le responsable d'un groupe de discussions pourrait être tenu d'insérer; à *l'action en cessation* aux fins d'obtenir l'ordre donné de faire cesser im-

322 P. GERARD et V. WILLEMS, « Prévention et répression de la criminalité sur Internet », *infra*, chap. 5.

médiatement la diffusion d'une information portant atteinte à l'honneur, à la bonne réputation...; *au droit d'accès et de rectification* en matière de données à caractère personnel, etc.

La présente étude se limite en définitive aux questions de responsabilité du chef d'informations illicites ou inexactes diffusées *via* Internet, en particulier dans le contexte des groupes de discussion et des serveurs.

4. Pour commencer, il n'est sans doute pas inutile de dissiper un certain nombre de malentendus véhiculés à propos du phénomène « Internet » (II.). A cet effet, on se propose d'identifier les « faux » et « vrais » problèmes suscités par le développement d'Internet.

Ensuite, il faut bien admettre qu'étant donné le caractère international du réseau des réseaux, loin d'être confronté à un prétendu « vide juridique », on est plutôt placé devant la difficulté de déterminer, parmi une pluralité de règles, celles qui ont vocation à s'appliquer à chaque cas d'espèce (III.). On ne peut donc éluder les questions classiques, mais néanmoins délicates, de conflits de juridictions et de lois en cas de litiges transfrontières.

Enfin, il y a lieu de s'interroger sur la substance des règles de responsabilité appelées à régir la diffusion d'informations illicites ou inexactes *via* Internet (IV.). Il convient à cet égard de prêter attention à la diversité des rôles assumés par les différents acteurs en présence.

II. Un besoin de clarification : pour une approche sereine et raisonnée du phénomène « Internet »

II.1. Démystifier Internet : les « faux » problèmes

5. Depuis quelques mois, la grande presse s'est emparée du thème Internet. On y observe une nette tendance à monter les problèmes en épingle, à partir de certains cas limites[323]. Ainsi, il est souvent affirmé qu'Internet peut véhiculer le meilleur comme le pire et qu'aucun usager n'est à l'abri du pire. Chacun des utilisateurs du réseau serait à tout moment un destinataire potentiel d'informations non désirées à caractère raciste, antisémite, pornographique... Sans être totalement dénuée de pertinence, pareille affirmation appelle cependant quelques nuances. En effet, quel que soit le service concerné, l'accès à l'information suppose un acte volontaire de la part de l'usager qui, dans une masse d'informations et d'images, peut choisir celles qu'il souhaite lire ou regarder.

L'abonnement à des forums de discussion est toujours volontaire. Certes, rien n'interdit à un abonné de poster un message étranger au thème du groupe. Toutefois, l'émetteur d'un message illicite sera, en principe, aisément identifiable. Ensuite, le modérateur du forum est chargé de « filtrer » les articles postés sur ce forum, de manière à retenir uniquement ceux qui correspondent aux objectifs du groupe. Enfin, la participation à un groupe de discussion ouvert et non modéré est également le résultat d'un choix conscient et libre.

Dans le cas des serveurs d'information, celle-ci est mise à la disposition des usagers. Mais, la décision d'aller chercher et lire ces informations leur appartient, sans que personne ne puisse la leur imposer. La possibilité d'accéder à des informations de nature pornographique ou pédophile est généralement subordonnée à la nécessité de payer le service offert, exigence à laquelle personne n'est tenu de satisfaire.

Reste le problème spécifique de la protection des mineurs face aux contenus dommageables (violents, à caractère pédophile...) véhiculés sur le *net*[324]. A ce égard, on fera remarquer que leurs parents (ou tuteurs légaux) assument la responsabilité de leurs actes. Par ailleurs, un contrôle peut

323 L'étude suivante nous a été très utile pour la rédaction de la présente section : A. U. I., « Pour une intégration sereine et un développement harmonieux d'Internet dans la société française ». Rapport du 7 juin 1996, disponible sur le site de l'A. U. I. (http://www.aui.fr).

324 Sur la question, voy. Commission européenne, Livre Vert sur la protection des mineurs et de la dignité humaine dans les services audiovisuels et d'information, COM (96) 483 et Communication au Parlement européen, au Conseil, au Comité économique et social et au comité des régions. Contenu illégal et préjudiciable sur Internet, COM (96) 487.

(doit) être exercé par les parents, enseignants et éducateurs afin de les protéger contre des contenus préjudiciables — même éventuellement licites, mais jugés nuisibles en fonction du type d'éducation qu'ils entendent leur donner. Enfin, des parades peuvent également être recherchées du côté des solutions techniques proposées par certains fournisseurs d'accès et/ou adoptées par des gestionnaires de réseau : blocage de l'accès à certains sites (système de la liste noire); limitation de l'accès à des sites spécifiés (système de la liste blanche, qui peut être mise en place, par exemple, au niveau des établissements scolaires ou des bibliothèques publiques...); restriction d'accès à des sites identifiés, de manière intuitive, à l'aide de mots clés prédéfinis[325]. Ces différents types de logiciels de filtrage peuvent présenter certains inconvénients et failles[326], ils ne dispensent donc pas les adultes de s'acquitter, avec sens des responsabilités, de leurs devoirs de surveillance et de vigilance. Quoi qu'il en soit, comme le souligne Michel Vivant (faisant allusion à la pédophilie), il ne serait pas sage de concevoir tout un « droit du *net* » à partir de l'un ou l'autre cas tout à fait exceptionnels, fussent-ils monstrueux[327].

Bref, dans la plupart des hypothèses, les informations reçues ont pu être sélectionnées, mieux encore que dans les médias audiovisuels classiques. Il est peu probable que l'utilisateur d'Internet soit placé, à son insu, en situation de destinataire d'informations non désirables.

6. Autre difficulté souvent évoquée : l'impossibilité d'identifier les auteurs de messages illicites. Sous couvert de *l'anonymat*, n'importe quel usager mal intentionné aurait la possibilité de diffuser, en toute impunité, des informations de la pire espèce.

Sans vouloir gommer toute difficulté, il importe de préciser que, pour pouvoir accéder à Internet, pratiquement tous les usagers, qu'ils aient la qualité d'émetteurs ou de récepteurs ou les deux, doivent passer par un fournisseur d'accès. Ce dernier connaît dès lors l'identité et l'adresse de tous les acteurs d'Internet et est donc apte à identifier ou à fournir à

325 Cf. le *Communication Decency Act* adopté aux Etats-Unis en février 1996 (déclaré anticonstitutionnel par une décision de la cour d'appel fédérale de Philadelphie en date du 12 juin 1996) et l'Amendement Fillon en France (déclaré contraire à la Constitution par une décision du Conseil Constitutionnel du 23 juillet 1996). Des trois dispositions introduites par cet amendement dans la loi n° 96-659 du 26 juillet 1996 sur la réglementation des télécommunications (*J. O.* du 27 juillet 1996, modifiant la loi du 30 septembre 1986 sur la liberté des communications), seules deux ont été déclarées contraires à la Constitution. Reste donc un article qui dispose : « Toute personne dont l'activité est d'offrir un service de connexion à un ou plusieurs services de communication audiovisuelle mentionnés au 1er alinéa de l'article 43 est tenue de proposer à ses clients un moyen technique leur permettant de restreindre l'accès à certains services ou de les sélectionner ».

326 Le choix de certains mots clés peut conduire à l'élimination de sites pourtant inoffensifs. Les surprises sont, par ailleurs, toujours possibles : il n'est pas exclu qu'une recherche effectuée à l'aide d'un mot clé anodin puisse conduire sur un site peu fréquentable... Pour une description et une évaluation des solutions techniques existantes et, en particulier, du standard PICS (« Platform for Internet Content Selection »), voy. la Communication précitée de la Commission européenne sur le *Contenu illégal et préjudiciable sur Internet*, COM (96) 487.

327 M. VIVANT, « Internet et modes de régulation », *infra*, chap. 8, n° 21.1.

l'autorité judiciaire les moyens d'identifier tout utilisateur à partir de l'adresse de sa machine.

Il faut dire aussi que la plupart du temps les émetteurs d'informations s'identifient clairement. Chacun sait que telle base de données ou tel serveur est placé sous la responsabilité d'une université, d'un centre de recherches, d'un organisme, d'une personne, physique ou morale... bien identifié. Il est vrai que l'auteur de messages gravement illicites a pu utiliser les services d'un logiciel permettant l'émission anonyme d'information (« ré-expéditeur anonyme », en anglais « anonymous remailer »). Cependant, les responsables de pareils services sont, quant à eux, identifiables et peuvent être contraints par l'autorité judiciaire d'aider à identifier l'émetteur d'origine.

Il reste qu'il sera parfois impossible d'identifier des auteurs de délits, mais Internet n'a pas le monopole de cette difficulté. En d'autres domaines, il arrive aussi que des enquêteurs échouent au plan de l'administration de la preuve, en sorte que les procédures d'instruction n'aboutissent pas et que les coupables demeurent impunis.

7. Un autre malentendu fréquent porte sur la notion de *censure*, brandie par certains pour stigmatiser toutes formes quelconques de contrôle considérées comme autant d'entraves à la liberté d'expression. On tente ainsi, par un emploi détourné du langage, de faire accroire que les libertés d'opinion, d'édition ou de presse devraient pouvoir s'exercer en toute impunité.

Cette fallacieuse conception procède, en réalité, d'une confusion entre deux formes d'intervention bien distinctes : la *censure* proprement dite, intervenant *a priori* et émanant d'une autorité quelle qu'elle soit, d'une part, et le contrôle ou la *sanction* susceptible de frapper *a posteriori*, d'autre part. Rares sont les contrôles *a priori* exercés aujourd'hui par l'autorité publique (ils n'existent plus en matière littéraire, seules les entreprises de radiodiffusion, de cinéma ou de télévision étant, le cas échéant, soumises à un régime d'autorisation). Peu nombreux sont, par ailleurs, les textes de loi visant à censurer, sous la menace de la sanction pénale, des contenus de pensée. Mais, cela ne signifie pas que les auteurs, penseurs, écrivains ou artistes jouissent d'une totale « immunité ». Comme le note, à juste titre, A. Strowel, « la censure s'opère au nom d'une idéologie (qu'elle soit d'Etat, religieuse, voire culturelle) qui heurte de front la liberté d'expression »[328]. Autre chose est l'obligation qui pèse sur tout un chacun de répondre des dommages causés à autrui en raison d'idées exprimées ou de propos tenus.

328 A. STROWEL, « Démêlés judiciaires autour d' « Une paix royale » de Pierre Mertens », obs. sous T. G. I. Paris (réf.), 22 septembre 1995, *J. T.*, 1996, p. 196.

8. Comme le suggère l'article 10 de la Convention de sauvegarde des droits de l'homme et des libertés fondamentales, l'exercice de la liberté d'expression, « qui comprend la liberté d'opinion et la liberté de recevoir ou de communiquer des informations et des idées », « [comporte] des devoirs et des responsabilités et peut être soumis à certaines formalités, conditions, restrictions ou sanctions, prévues par la loi, qui constituent des mesures nécessaires dans une société démocratique, à la sécurité nationale, à l'intégrité territoriale ou à la sûreté publique, à la défense de l'ordre et à la prévention du crime, à la protection de la santé ou de la morale, à la protection de la réputation ou des droits d'autrui, pour empêcher la divulgation d'informations confidentielles ou pour garantir l'autorité et l'impartialité du pouvoir judiciaire ».

On n'aurait pu mieux dire. En d'autres termes, nous sommes non pas en régime de *licence*, mais en régime de *liberté*, qui implique certaines limites — celles nécessaires à la sauvegarde de la liberté des autres —, limites dont la transgression entraîne une *responsabilité*.

Il ne fait pas de doute que chacun des usagers d'Internet est tenu de se comporter en « bon père de famille » et se trouve soumis aux règles de responsabilité (civile et pénale) du droit commun. Lorsque la victime est un tiers par rapport à l'émetteur d'une information litigieuse (inexacte ou illicite), elle pourra assigner ce dernier, en droit belge, sur la base des articles 1382 et 1383 du Code civil. Dans d'autres hypothèses, c'est l'utilisateur créancier de l'information, au titre d'un contrat d'accès, qui est la victime de données non conformes à son attente légitime (compte tenu de leur nature ou des stipulations du contrat). Elle pourra alors envisager de situer son action sur le terrain de la responsabilité contractuelle. Enfin, dans le cas où une information est à l'origine d'une atteinte à l'intégrité physique de l'utilisateur, se pose la question de savoir, dans le cadre de l'Union européenne, si l'action en responsabilité du fait des produits défectueux contre le producteur de la base de données est envisageable[329].

II.2. Les spécificités d'Internet : les « vrais » problèmes

9. Internet n'est pas un « super-réseau », mais une vaste structure, de couverture mondiale, constituée d'une multitude de réseaux locaux, régionaux... interconnectés. Un langage de communication commun (les protocoles de la famille « TCP/IP »), assure l'interopérabilité des machines hétérogènes reliées au réseau, leur permettant ainsi de dialoguer entre elles.

329 Sur cette question, voy. notre thèse *Bases de données et informations inexactes*, 1996, deuxième partie, à paraître.

Les spécificités essentielles d'Internet tiennent aux caractéristiques de son infrastructure et de son mode de fonctionnement. Il s'agit d'une architecture *distribuée* (il n'y a donc *pas un point unique de contrôle*) et *redondante* : son *maillage* est tel qu'il est pratiquement impossible de déterminer *a priori* le chemin qu'emprunteront les données pour être acheminées d'un point à l'autre[330]. De plus, s'agissant du WWW, les points d'entrée sur un site Web peuvent être multiples par le jeu des *hyperliens*, qui permettent, grâce à un simple « clic », de naviguer d'un site ou d'un serveur à l'autre. Il en résulte une réelle difficulté de contrôle de la part des serveurs et fournisseurs d'accès. Il leur est pratiquement impossible d'opérer une vérification systématique de tous les messages qu'ils relayent. La suppression d'un site est vaine, étant donné l'aisance et la rapidité avec lesquelles il peut être déplacé pour être hébergé sur un serveur distinct. De même, la fermeture d'un accès peut rester sans effet dans la mesure où les utilisateurs ont toujours le loisir d'atteindre le serveur interdit *via* d'autres sites qui, eux-mêmes y donnent accès.

10. L'évolution rapide des techniques, l'instabilité des usages et le renouvellement constant des procédures et « astuces » en tout genre permettant de contourner les « interdits » constituent autant d'obstacles à la réflexion juridique et à l'adoption de dispositifs normatifs efficaces destinés à régir Internet. A ce stade, les juristes doivent, à notre avis, adopter une position attentiste. Leurs analyses — et la nôtre — ne peuvent être que provisoires et limitées, en attendant de nouveaux développements et une compréhension plus profonde du phénomène d'ensemble. Il s'agit de prendre l'exacte mesure des problèmes avant toute intervention contraignante.

11. Enfin, un des défis majeurs pour le droit découle du caractère international du réseau Internet. Aux questions classiques de loi applicable, de juridiction compétente et d'exécution extra-territoriale des décisions de justice, s'ajoutent certaines difficultés inhérentes aux traits spécifiques du réseau. Internet recèle, en effet, de réelles possibilités de contourner les règles établies par un Etat. Il est relativement facile de délocaliser des informations de manière à éviter qu'elles ne se trouvent physiquement sur un territoire où elles seraient illégales.

12. En résumé, les véritables difficultés spécifiques suscitées par Internet dans l'application du droit sont liées à la *nature particulière de son maillage*, à la *fugacité des messages*, à *l'évolution très rapide des techniques* et au *caractère transnational du réseau des réseaux*.

330 Technique du « packet switching » : les informations sont découpées en « paquets » qui, pour être acheminés de A vers B, n'empruntent pas forcément la route A—B. Si cette dernière est encombrée ou impraticable, les paquets d'informations peuvent être aiguillés vers d'autres chemins : A—C—B ou A—D—B ou A—C—D—B, etc. On précise aussi que les différents paquets peuvent être acheminés sur des routes distinctes, l'ensemble d'informations de départ étant reconstitué à l'arrivée.

III. Cyberespace, abolition des frontières et droit applicable

III.1. La détermination de la loi applicable

13. L'accès à un site ou à une base de données est parfois subordonné à la conclusion — en dehors du réseau — d'un contrat d'abonnement. L'hypothèse se rencontre de plus en plus fréquemment s'agissant d'informations à haute valeur ajoutée. Mais il arrive aussi que les usagers puissent accéder librement aux sites et bases de données disponibles sur le réseau. Dans ce cas, l'existence d'un contrat n'est pas nécessairement exclue, même si l'utilisateur n'a pas le sentiment d'être en relation contractuelle avec le producteur[331]. En effet, les pages-écran qu'il visualise au cours de sa navigation peuvent contenir un ensemble de dispositions susceptibles d'être considérées comme une offre de contracter. On peut donc estimer qu'un contrat s'est formé dès acceptation de pareille offre, manifestée notamment par la poursuite de l'interrogation. Il découle de ces considérations que l'action en responsabilité introduite par le destinataire victime d'une information non conforme pourra être de nature contractuelle.

14. En principe, il est loisible aux parties de choisir de commun accord la loi applicable à leur relation. Une telle indication peut figurer sur une page-écran, même s'il n'est pas évident de prouver ultérieurement que l'utilisateur en a eu connaissance et a donné son consentement sur ce point précis. Le principe du choix par les parties de la législation applicable au contrat est consacré par la Convention de Rome du 19 juin 1980 sur la loi applicable aux obligations contractuelles, qui a été transposée en droit belge par la loi du 14 juillet 1987. Si aucune loi n'a été choisie, le contrat est régi par la loi du pays avec lequel il présente les liens les plus étroits[332]. A cet égard, il est présumé que ce critère vise le pays où la partie qui doit fournir la prestation caractéristique a, au moment de la conclusion du contrat, sa résidence habituelle ou son principal établissement (art. 4). En matière de fourniture d'information, il s'agit vraisemblablement du lieu d'établissement de l'animateur d'un site Web, d'un serveur d'information ou d'un groupe de discussion...

331 Cf. M. VIVANT, C. LE STANC et alii, *Lamy droit de l'informatique*, 1995, p. 1176, n° 1798.

332 Si le contrat est conclu entre un professionnel et un consommateur, le libre choix des parties dans la détermination de la loi applicable ne peut avoir pour résultat de priver le consommateur de la protection que lui assurent des dispositions impératives de la loi du pays dans lequel il a sa résidence habituelle. Pour d'autres précisions, lire l'article 5 de la loi du 14 juillet 1987.

15. En matière délictuelle, la loi la plus volontiers désignée est celle du lieu de commission du délit (la *lex loci delicti*). Ainsi, supposons qu'à partir du territoire de la Belgique, un individu propage une information mensongère sur telle société commerciale dont le siège est situé en Norvège, ce qui entraîne une chute instantanée de sa cotation en bourse. Pour déterminer l'importance et le type de réparation due, le tribunal saisi appliquera, en principe, la loi de l'Etat où est localisé l'émetteur, en l'occurrence la loi belge.

La localisation du lieu de commission d'un délit *via* Internet n'est pas nécessairement aisée à identifier car un message peut être envoyé au moyen d'un ordinateur situé dans un pays pour être diffusé par une machine localisée à un autre coin du globe. Il existe cependant des possibilités de « tracer » l'information pour remonter à sa source. Souvent aussi, un message illicite émis en un point a pu être reçu en divers points situés éventuellement dans des pays différents. Les solutions de la jurisprudence sont fluctuantes en la matière : est retenue tantôt la loi du fait dommageable tantôt la loi de réalisation du dommage. Pourquoi ne pas laisser à la victime le choix de la loi applicable ? Par ailleurs, ne peut-on concevoir que réparation soit demandée par plusieurs victimes chaque fois par référence au droit du pays où elles résident ?

En droit belge, la jurisprudence considère, depuis l'arrêt *Bologne* de la Cour de cassation en date du 17 mai 1957, que les lois de police, au nombre desquelles on range les lois qui déterminent les éléments du fait générateur de la responsabilité délictuelle ou quasi-délictuelle ainsi que le mode et l'étendue de la réparation, sont applicables aux faits commis sur le territoire du Royaume, quelle que soit la nationalité de leur auteur (art. 3, al. 1 C. civ.)[333]. Ce rattachement de la matière de la responsabilité fondée sur les articles 1382 et suivants du Code civil aux lois de police conduit à l'application de la loi du pays où a été commis le fait générateur de cette responsabilité. Cette solution prévaut également si le délit est commis dans un autre pays que celui où le dommage est subi. Cependant, à plusieurs reprises, la Cour de cassation de Belgique semble avoir admis une ouverture en faveur d'un rattachement, à titre subsidiaire, de la responsabilité civile extra-contractuelle à l'autonomie de la volonté. Autrement dit, les parties auraient le loisir de déterminer le droit applicable à l'action délictuelle[334].

333 Cf. Cass., 17 mai 1957, *R. C. J. B.*, 1957, p. 92.

334 Ainsi pourraient-elles s'entendre, après la survenance du litige, pour choisir de commun accord la loi appelée à régir l'action. L'observation du droit belge accrédite l'impression que la règle de conflit de lois en matière de responsabilité civile pourrait évoluer dans un proche l'avenir. A ce propos, voy. M. FALLON, « L'incidence de l'autonomie de la volonté sur la détermination du droit applicable à la responsabilité non contractuelle », in *Mélanges Roger O. Dalcq. Responsabilités et assurances*, Bruxelles, Larcier, 1994, pp. 159-187, et les réf. citées.

16. En matière pénale, il est prévu que la loi belge est applicable aux infractions commises sur le territoire du Royaume, par des Belges ou par des étrangers (art. 3 du Code pénal). C'est le principe, bien connu, de territorialité du droit pénal : dès que quelqu'un, peu importe sa nationalité, commet une infraction sur le territoire de la Belgique, il peut être poursuivi et le juge saisi statuera selon le droit belge.

Au plan pénal, les questions de loi applicable et de juge compétent sont donc étroitement liées.

III.2. La détermination du juge compétent

17. La jurisprudence considère que le juge belge est compétent pour statuer sur une infraction dès l'instant où un de ses éléments constitutifs a été commis en Belgique. En revanche, aux termes de l'article 4 du Code pénal, « l'infraction commise hors du territoire du Royaume par des belges ou par des étrangers n'est punie en Belgique que dans les cas déterminés par la loi »[335]. Sauf circonstances exceptionnelles (atteintes à la sûreté de l'Etat...), les infractions commises à l'étranger ne sont poursuivies que si l'inculpé est appréhendé en Belgique. Souvent aussi, la compétence du juge est soumise au principe de la double incrimination.

Supposons qu'un message à caractère raciste ou incitant à la violence soit « lancé » sur le réseau à partir de l'Allemagne et reçu en Belgique. On peut penser que, dans ce cas, l'incitation à la haine ou à la violence est réalisée en Belgique de sorte qu'un élément constitutif de l'infraction est bien localisé sur le territoire du Royaume. Le juge belge est donc compétent pour statuer sur l'infraction, sur le fondement de l'article 3 du Code pénal, ce qui signifie que les conditions plus strictes de l'article 4 (double incrimination, présence de l'inculpé sur le territoire du Royaume...) ne doivent pas être remplies. Cette solution peut s'autoriser, par analogie, de différentes décisions relatives au domaine audiovisuel. En effet, des juridictions ont estimé, dans le cas d'infractions commises à la radio ou à la télévision, que « l'infraction est supposée accomplie en tout lieu où pareille diffusion a pu être reçue ou entendue »[336].

18. Pour la détermination du juge compétent, en matière civile, on se référera, en Europe occidentale, aux principes inscrits dans la Convention de Bruxelles du 27 septembre 1968, pour autant que le pays de chacune des parties en litige ait signé cette Convention.

335 Cf. les articles 6 à 14 du Code de procédure pénale, ainsi que certains traités internationaux signés par la Belgique.

336 Cf. J. -P. BUYLE et O. POELMANS, « Internet : quelques aspects juridiques (suite) », n° 17, à paraître dans le D. I. T. Voir, par exemple, Bruxelles (Ch. Mises Acc.), 5 décembre 1991, *J. T.*, 1992, p. 387.

Les parties à un contrat peuvent convenir de commun accord du tribunal compétent pour statuer (art. 17 et 18). A défaut, il s'agira du tribunal de l'Etat dans lequel le défendeur est domicilié ou dispose de son siège social (art. 2). Encore qu'en matière de responsabilité contractuelle, le défendeur peut également être attrait devant le tribunal où l'obligation a été ou doit être exécutée (art. 5, 1°).

En matière délictuelle ou quasi-délictuelle, il est prévu, aux termes de l'article 5, 3° qu'est compétent le tribunal du lieu où le fait dommageable s'est produit. Cette notion de « lieu où le fait dommageable s'est produit » a déjà été interprétée par la C. J. C. E. , qui laisse le choix au demandeur d'agir soit dans le pays où le fait générateur s'est produit, soit dans celui où le dommage est survenu[337]. On en déduit qu'un utilisateur d'Internet peut assigner l'émetteur d'une information qui lui a causé un dommage soit devant un tribunal situé dans le pays d'où a lieu l'émission, soit devant le tribunal du lieu où est reçue l'information à l'origine de son préjudice.

Cette solution rejoint le système de droit commun, valable en dehors de l'espace européen, qui retient pareillement la compétente du tribunal du lieu du délit (soit le juge belge pour un délit localisé en Belgique...) ou celle du juge du lieu du domicile ou du siège social du défendeur[338].

III.3. L'exécution extra-territoriale des décisions de justice

19. En Europe, les Conventions de Bruxelles du 27 septembre 1968 et de Lugano du 16 septembre 1988 rendent l'*exequatur* des décisions de justice étrangères quasi automatique, sous la réserve de l'ordre public. Il peut arriver que l'*exequatur* soit refusé dans des matières où les sensibilités varient d'un pays à l'autre, comme c'est souvent le cas en ce qui concerne précisément la liberté d'expression. Mais, comme le souligne, à juste titre, M. Vivant, « cela ne traduirait nullement une impuissance du droit à prendre en charge les réseaux, puisqu'il ne s'agit ici que de droit commun »[339].

En dehors de l'Europe, la question de l'*exequatur* trouve des réponses nettement moins assurées. Les différences entre les systèmes juridiques sont telles — l'on songe aux pays européens, à la Chine, au Vietnam, à la Thaïlande, à Singapour, à l'Iran, à l'Algérie... — que les refus d'*exequatur*

337 C. J. C. E., 30 novembre 1976, aff. 21/76, *Recueil*, 1976, p. 1735; C. J. C. E., 7 mars 1995, *J.T.D.E.*, 1995, p. 85; Comm. Bruxelles, 4 juin 1985, *R. D. C.*, 1986, p. 393.

338 A ce propos et pour plus de détails, M. VIVANT, « Cybermonde : Droit et droits des réseaux », *J.C.P.*, G, 1996, I, 3969, p. 404, n° 12.

339 M. VIVANT, *Ibidem*, p. 405, n° 16.

ne sont pas à exclure. En matière pénale, l'efficacité à l'étranger des décisions rendues dans un Etat est encore plus incertaine. On signale toutefois que des accords existent entre pays pour régler la mise en oeuvre de l'extradition.

A noter enfin qu'il existe aussi des procédures internationales de coopération relative à la recherche d'infractions, telle la Recommandation n° 95/13 du Conseil de l'Europe afin de favoriser les enquêtes, perquisitions et saisies en environnement informatique transfrontalier.

IV. Le partage des responsabilités entre les divers intervenants

IV.1. Les principes clés d'un « système de responsabilité »

20. On examine à présent les principes susceptibles de guider aussi bien les acteurs d'Internet que la jurisprudence dans l'évaluation de la responsabilité des premiers.

Avant d'entrer dans le vif du sujet, il n'est pas superflu de formuler deux remarques.

Dès lors qu'un utilisateur est lié par un contrat à un fournisseur d'information — peu importe, du reste, qu'il ait été conclu en dehors du réseau ou se soit noué par voie électronique —, il sera fondé à rechercher la responsabilité de ce dernier par référence au contrat s'il a subi un dommage résultant de la non conformité de l'information reçue[340].

Par ailleurs, il importe de ne pas perdre de vue l'importance des contrats passés entre certains acteurs d'Internet. En effet, plusieurs questions peuvent y être réglées, notamment l'obligation faite à une partie d'effectuer certains contrôles. Ainsi, dans ses relations contractuelles avec les utilisateurs, un fournisseur d'accès peut prendre l'engagement de ne pas donner accès à certains types de serveurs et, partant, s'obliger à vérifier les contenus. De même, le contrat unissant l'éditeur à un service d'hébergement peut contenir des obligations relatives à la protection des mineurs ou des consommateurs... Dans ces deux hypothèses, les acteurs concernés assument volontairement un niveau plus élevé de responsabilité à l'égard de leurs abonnés et celle-ci pourra, le cas échéant, être mise en cause dans un cadre contractuel.

21. Ces précisions apportées, il est permis d'aborder la délicate question portant sur l'imputation de la responsabilité. Faut-il rendre responsable le serveur qui fournit l'information, le fournisseur d'accès, simple intermédiaire technique chargé de permettre l'accès au réseau, l'opérateur qui loue ses lignes de télécommunication ou l'auteur du message, dont il n'est pas toujours aisé d'établir l'identité ?

---

340 Mais il se peut qu'une information conforme au point de départ ait été déformée par la suite, par exemple à l'occasion de son transport. Sans être fréquente, l'hypothèse ne peut cependant pas être totalement écartée. Est ainsi posée la question de la responsabilité des opérateurs de réseau. A ce sujet, voy. notre thèse précitée, n° 241.

L'attention s'est surtout focalisée sur les fournisseurs d'accès (FA) comme en témoigne la jurisprudence, encore mince, disponible en la matière[341]. Certains préconisent, en effet, de responsabiliser au maximum les FA. Ils tirent argument de la circonstance que l'auteur d'un message litigieux oeuvre souvent à partir de l'étranger et est, de surcroît, difficile à identifier, alors que le FA est généralement proche de l'usager ayant subi un dommage. De façon générale, on fait aussi valoir que, pour accéder à Internet et être reconnu sur le réseau, tout utilisateur a dû se faire attribuer une adresse, se déclarer auprès d'une personne accréditée, en l'occurrence un FA. Celui-ci serait donc le mieux à même de jouer un certain rôle de police, assorti d'une haute responsabilité. De leur côté, nombre de FA soulignent que, bien souvent, ils ne sont pas eux-mêmes fournisseurs de services et qu'il leur est pratiquement impossible de contrôler et, au besoin, de filtrer, les contenus offerts aux abonnés.

L'imputation systématique de la responsabilité aux FA ne nous semble pas la bonne voie. Nous sommes plutôt d'avis de tenir pour responsable, au premier chef, la personne qui prend l'initiative de mettre en ligne l'information. Peut également être déclaré responsable tout qui a une certaine prise sur l'information, c'est-à-dire qui a les moyens de la contrôler et à ce titre aurait pu ou dû intervenir et s'en est pourtant abstenu. Par application du droit commun de la *responsabilité civile*, on peut considérer que, dans ces circonstances, une négligence a été commise, dont son auteur doit pouvoir répondre. Mais, la plasticité des principes gouvernant la responsabilité civile est telle qu'il n'est pas exclu que les juges se montrent plus sévères, en imposant aux FA des obligations plus lourdes afin de favoriser l'indemnisation de la victime (notamment lorsque l'auteur du délit est éloigné). Il est certain, en revanche, que par application des principes généraux du *droit pénal*, un acteur d'Internet n'engage sa responsabilité que s'il est prouvé qu'il a matériellement, mais aussi délibérément (*sciens et volens*), commis un acte incriminé.

22. Dans la louable intention d'éviter « de faire porter l'entière responsabilité de l'ensemble des maux des réseaux » sur les FA, d'aucuns[342] préconisent de transposer au cas des réseaux, quel que soit le type de message litigieux (infraction de presse ou non), le régime de responsabilité en cascade instauré dans le domaine de la presse écrite et étendu à l'audiovisuel par la loi (en France, par exemple[343]) ou par certaines décisions de jurisprudence (en Belgique[344]).

341 Cf. les décisions citées et commentées *infra*. On rappelle aussi que fin 1995, Compuserve a dû suspendre temporairement l'accès à plus de 200 forums sur ordre des autorités allemandes.

342 F. OLIVIER et E. BARBRY, « Des réseaux aux autoroutes de l'information : révolution technique? Révolution juridique? 2. Du contenu informationnel sur les réseaux », *J. C. P.*, G, 1996, I, 3928, p. 185, n° 43.

343 En France, la responsabilité éditoriale a été instaurée pour la presse écrite par la loi du 29 juillet 1881, étendue aux services de communication audiovisuelle par la loi du 29 juillet 1982, et maintenue en vigueur par la loi du 30 septembre 1986 relative à la liberté de communication. Pour assumer cette responsabilité, le directeur de la publication doit être à même de contrôler les messages diffusés. D'où la nécessité légale d'un enregistrement préalable à la communication au public (cf. art. 93-3 de la loi du 29 juillet 1982, introduit par la loi du 13 décembre 1985). Pour ce qui est de la télématique, la jurisprudence considère que seuls les services de bases de données, dont le contenu est préenregistré, sont susceptibles d'engager la responsabilité pénale du directeur de la publication.

344 Quelques arrêts et jugements récents du ressort de la Cour d'appel de Bruxelles estiment que le régime de responsabilité en cascade prévu par l'article 25, alinéa 2 de la Constitution pour la presse écrite s'applique également à l'audiovisuel (Cf. Bruxelles, 19 février 1985, *R. W.*, 1985-1986, 806, note J. CEULEERS; Bruxelles, 7 juin 1991, *Rev. dr. pén. crim.*, 1992, p. 131; Bruxelles, 25 mai 1993, *J. T.*, 1994, p. 104, obs. F. JONGEN). Cependant, la Cour de cassation et la doctrine restent prudentes à l'égard de cette jurisprudence minoritaire. L'interprétation du texte en néerlandais de la Constitution, qui parle de *druk pers* (presse imprimée), semble faire obstacle à l'élargissement à l'audiovisuel du régime de faveur prévu pour la presse. Pour un examen d'autres arguments, voy. F. JONGEN, « La responsabilité pénale et civile de la presse », *Journal des procès*, 1991, p. 11. Cf. aussi les références citées par F. TULKENS et M. VAN DE KERCHOVE, *Introduction au droit pénal*, 2e éd. revue et mise à jour, A la rencontre du droit, Bruxelles, E. Story-scientia, 1993, p. 199 et par C. HENNAU et J. VERHAEGEN, *Droit pénal général*, 2e éd. revue et mise à jour, Travaux de la Faculté de Droit de l'U. C. L., Bruxelles, Bruylant, 1995, p. 68, n° 58.

On précise aussi qu'un récent arrêt de la Cour de cassation (du 31 mai 1996, *J. T.*, 1996, p. 597) a confirmé sa jurisprudence, établie depuis un arrêt du 24 janvier 1863, selon laquelle le régime de la responsabilité en cascade s'applique tant à l'action civile qu'à l'action pénale. On sait qu'une controverse existait de longue date sur cette question. A ce propos, voy., par exemple, F. TULKENS et M. VAN DE KERCHOVE, *Ibidem*, p. 191 et les réf.; C. HENNAU et J. VERHAEGEN, *Ibidem*, p. 66, n° 57 et les réf.; R. O. DALCQ, *Traité*, 1967, p. 420, n° 1246.

345 I. FALQUE-PIERROTIN (sous la présidence de), *Rapport de la Mission Interministérielle sur l'Internet*, 16 juin 1996, pp. 59-60.

Ainsi, en ce qui concerne Internet, et en raisonnant par référence au droit belge, le premier maillon de la chaîne pourrait être l'auteur, et à défaut serait retenue la responsabilité de plein droit et automatique, de l'éditeur (le responsable éditorial : fournisseur de service ou animateur d'un groupe de discussion), à défaut le serveur, à défaut le fournisseur d'accès et enfin, à défaut, le transporteur. D'autres types de hiérarchie des responsabilités sont évidemment concevables, sans compter qu'il est aussi possible d'exclure certains maillons de la cascade.

Ce système présente au moins quatre avantages : 1°) les victimes sont pratiquement assurées de trouver toujours un responsable; 2°) l'automatisme de la cascade en facilite la mise en oeuvre par le juge, ce qui permet d'éviter de longues procédures judiciaires; 3°) uniformisation du régime et des contrôles applicables à tous les messages quel que soit le support d'accès (presse, audiovisuel, réseaux numériques); 4°) la présomption étant réfragable, la personne mise en cause peut toujours la renverser.

A l'instar du rapport de la Mission Interministérielle sur l'Internet, présidée par Madame Falque-Pierrotin, nous sommes enclins à préférer le système de responsabilité de droit commun[345]. Il ne nous paraît pas souhaitable, et en tout cas prématuré, de faire peser une responsabilité automatique, même par défaut, sur les acteurs d'Internet, et singulièrement sur les opérateurs, serveurs et fournisseurs d'accès. Comme le souligne le rapport, le risque est grand de voir une grande partie de l'activité en ligne

quitter le territoire national vers des pays dont la législation est moins sévère. En outre, le régime de responsabilité éditoriale suppose une réelle possibilité de contrôler les informations diffusées, ce qui est le cas en matière de presse écrite, alors qu'en revanche, les acteurs cités ne disposent que de moyens limités de vérification des contenus. Enfin, dans un environnement ouvert comme Internet, les rôles sont moins définis, volatiles, et les liens existants entre les acteurs moins nets.

Ces caractéristiques apparaissent comme autant d'obstacles à l'adoption, pour la communication sur Internet, d'un système visant à la désignation préalable et automatique des responsables. Plus fondamentalement, il peut sembler paradoxal de vouloir étendre, d'abord à l'audiovisuel et ensuite aux réseaux, un régime actuellement fort remis en question[346] et qui vise, du reste, à une « déresponsabilisation »[347], alors que l'on prétend ici, tout au contraire, renforcer la responsabilité des acteurs d'Internet.

Le droit commun de la responsabilité se révèle, en définitive, plus souple et plus conforme au principe de liberté : les intermédiaires techniques sont moins pressés de surveiller, *a priori*, tous les messages, mais ils restent tenus, de faire diligence pour empêcher la diffusion de messages illégaux ou pour éliminer les informations litigieuses dont l'existence leur serait signalée ou qu'ils auraient pu et dû découvrir par eux-mêmes. La référence au seul droit commun implique qu'*au plan pénal*, *tous* les acteurs d'Internet peuvent être poursuivis comme auteurs principaux, coauteurs ou complices, s'ils ont sciemment mis (ou contribué à mettre) à la disposition du public des informations illicites. Au plan civil, elle permet pareillement la mise en cause de *tous* les acteurs, la diligence due par chacun d'eux pouvant être appréciée, le cas échéant, avec plus ou moins rigueur, en fonction des circonstances d'espèce et/ou de l'évolution, constatée, du contentieux (voir *infra*).

Ces principes posés, il convient à présent d'apporter des précisions et des nuances, notamment à la lumière de la jurisprudence. On se propose d'aborder les questions, acteur par acteur, ce qui ne doit pas faire oublier qu'un acteur peut assumer plusieurs rôles (ainsi, un FA est parfois aussi serveur et/ou fournisseur de services; un utilisateur peut être en position de récepteur mais aussi, bien souvent, d'émetteur...).

346 Voy., par exemple, F. JONGEN, « La responsabilité pénale et civile de la presse », *op. cit.*, p. 11 et s.; H. -D. BOSLY, « Les relations entre la justice et la presse. Aspects de droit pénal et de droit de la procédure pénale », *Justice et médias. Trois avis préliminaires à la demande du Ministre de la Justice*, 1995, p. 29-30.

347 En effet, le régime de responsabilité en cascade a été instauré afin d'empêcher la censure indirecte que des éditeurs ou imprimeurs pourraient être tentés d'exercer sur les auteurs par crainte d'une action judiciaire.

IV.2. Applications et précisions

IV.2.1. Les fournisseurs d'information

23. Les fournisseurs d'information présentent divers visages. Sur Internet, tout le monde peut, en fait, devenir un fournisseur d'information. Tout usager disposant d'un ordinateur et des logiciels appropriés peut envoyer du courrier électronique ou mettre en place un groupe de discussion.

L'utilisateur, en position d'émetteur d'une information, assume une responsabilité pour le contenu. En principe, il est identifiable. Soit directement car il fournit une signature. Soit indirectement car les informations de routage permettent, en principe, de « tracer » le cheminement des données et de remonter ainsi à la source. A partir de l'adresse de la machine utilisée, il est d'ordinaire possible de déterminer l'identité de son titulaire : son fournisseur d'accès possède l'information et peut être contraint par une autorité judiciaire de la fournir.

Il ne sera pas toujours possible d'identifier l'auteur d'un délit. Ainsi, un individu peut lancer sur le réseau une information à caractère raciste au départ de la machine d'un autre ou d'une machine mise à disposition d'une multitude d'utilisateurs au sein d'un organisme, personne morale : une entreprise, une université, une administration. Mais, dans ce cas, la responsabilité (civile, à tout le moins) peut incomber, le cas échéant, au maître du réseau local, soit à la personne morale, sans préjudice pour elle d'exercer un recours contre l'auteur de l'acte illicite. Ainsi, les employeurs sont responsables des comportements de leurs employés dans l'usage d'Internet. D'où la nécessité de prendre un certain nombre de précautions, sur les plans technique et organisationnel, pour empêcher, autant que possible, les comportements délictueux. Sur le plan juridique, le contrat d'emploi (ou une éventuelle *acceptable use policy* qui y serait annexée) peut contenir des dispositions relatives aux prérogatives et devoirs des employés dans l'usage des moyens informatiques dont ils disposent.

Aux Etats-Unis et au Canada, de nombreuses institutions universitaires ont adopté des politiques et des règles définissant les droits et obligations de ceux qui font usage des capacités informatiques disponibles au sein des institutions[348].

Le même type d'analyse prévaut en ce qui concerne les groupes de discussion, appelés encore « listes » ou « babillards ». Ils permettent aux usagers de « poster » des informations rendues ainsi accessibles aux autres usagers. Ils sont soit ouverts, c'est-à-dire accessibles à tous les usagers du réseau, soit fermés, c'est-à-dire accessibles sur invitation ou moyennant

348 Pour des exemples, voy. P. TRUDEL, « La protection des droits et des valeurs dans la gestion des réseaux ouverts », p. 12 (http://www.droit.umontreal.ca/CRDP/).

certaines conditions. En toute hypothèse, il est difficile d'exclure la responsabilité du maître de la liste ou du groupe dès l'instant où il exerce un pouvoir de contrôle et de décision sur l'affichage des messages.

IV.2.2. Les fournisseurs d'accès et serveurs

24. Lorsque l'émetteur n'a pu être identifié, la tentation est grande de vouloir mettre en cause la responsabilité du FA. Comme les serveurs, les FA peuvent être tenus pour responsables s'ils diffusent des informations illicites. Encore faut-il qu'ils aient eu connaissance du contenu du message.

A notre sens, lorsque les FA ou serveurs agissent comme de simples intermédiaires techniques, sans exercer aucun contrôle éditorial, alors ils ne sont pas tenus de vérifier, de façon systématique (est-ce d'ailleurs possible ?) le contenu des informations qu'ils relayent[349]. Leur responsabilité ne pourra être engagée que s'ils étaient ou devaient raisonnablement être au courant de la teneur d'un message, étant donné la taille du système informatique du serveur ou du FA et du degré de contrôle qu'il leur permettait d'effectuer ou s'ils avaient été averti de la présence d'informations illicites... Cette manière de raisonner apparaît dans diverses décisions de justice.

Ainsi, dans l'affaire, souvent citée, *Cubby v. Compuserve*[350]. Le réseau Compuserve était poursuivi comme co-défendeur dans une action en diffamation pour avoir donner accès à des informations diffamatoires contenues dans une lettre d'information électronique (intitulée « Rumorville USA ») publiée par un abonné du réseau qui n'avait aucun autre lien avec Compuserve.

Compuserve a été exonéré de toute responsabilité au motif qu'il ne pouvait avoir connaissance du caractère dommageable de l'information transmise. Toutefois, est-il précisé, lorsque le réseau acquiert connaissance du caractère dommageable d'informations qui y sont véhiculées, il lui incombe de faire le nécessaire pour qu'elles soient retirées.

Le juge Peter K. Leisure a appliqué, en l'espèce, la technique de « l'équivalence fonctionnelle ». Il a fait valoir que Compuserve n'exerce

349 Ces principes rejoignent ceux avancés en France à propos du serveur en matière télématique. Ainsi, la Cour de cassation a eu l'occasion d'affirmer le principe de neutralité du centre serveur quant au contenu des messages, sauf preuve contraire d'un manquement à cette obligation de neutralité : « Attendu que statuant sur les poursuites dirigées contre Louis Roncin en sa qualité de responsable d'un centre serveur, la juridiction d'appel retient que celui-ci est un 'outil... entre les mains du fournisseur de services qui, seul, doit assumer la responsabilité des décisions à prendre quant à la validation ou à la non-validation des messages'; qu'elle ajoute qu'il n'est pas possible d'envisager que le directeur d'un tel centre — lequel « héberge » souvent des dizaines de services — assure une responsabilité quelconque quant au contenu des messages. Attendu qu'en l'état de ces énonciations, dont elle a fait application à Louis Roncin, la cour d'appel a justifié sa décision » (Cass. (ch. crim.), 15 novembre 1990, *Expertises*, n° 135, 1991, p. 24).

350 Cubby Inc. v. Compuserve Inc., 776 F. Supp. 135 (S. D. N. Y. 1991).

pas davantage de contrôle éditorial qu'une bibliothèque publique, une librairie ou un kiosque à journaux, dans la mesure où il est impossible pour ce fournisseur d'examiner le contenu de chaque publication. Sa responsabilité ne peut être engagée que si son ignorance est due à une négligence : le fait de ne pas avoir surveillé des abonnés apparemment suspects (ayant déjà été condamnés)...[351]

Une décision d'un tribunal néerlandais du 12 mars 1996 précise, dans le même ordre d'idées, que le FA mis en cause ne faisant qu'offrir des moyens permettant de porter à la connaissance du public des services, ne pouvait être tenu pour responsable du contenu desdits services, sauf si la situation lui était connue et qu'il en avait été informé[352].

Il ressort de plusieurs décisions françaises que le *comportement positif* d'intermédiaires techniques (FA et serveurs) est déterminant. Ainsi, une ordonnance de référé rendue par le T. G. I. de Paris le 12 juin 1996 a pris en considération les moyens mis en place par les FA pour informer et sensibiliser leurs abonnés. En l'espèce, sept FA avaient été assignés en justice par l'Union des Etudiants Juifs de France pour qu'il leur soit ordonné, sous astreinte, d'empêcher toute connexion, à partir de leur serveur d'accès, à des sites diffusant des informations à caractère révisionniste[353]. Dans diverses affaires, des juridictions ont pris en considération la circonstance que le défendeur avait procédé à la destruction de fichiers[354] ou effacé les informations litigieuses relayées sur son serveur[355]. Un défen-

351 En revanche, si un FA prétend à un certain contrôle éditorial et est dès lors assimilable à un « éditeur primaire » au sens du droit américain, il est censé connaître ce qui est publié. Divers critères permettent d'établir cette circonstance : par exemple, si on peut prouver que le FA censure, de fait, des messages ou s'il spécifie que ses publications « à destination des familles » sont « nettoyées » de tout matériel outrageant.

C'est ce qui ressort de l'affaire Prodigy. La firme de courtage Stratton Oakmont avait introduit une action en justice contre le fournisseur de services Prodigy, spécialiste de l'information financière *on line*, et un usager anonyme, au motif qu'un message posté sur le « bulletin board » (« babilleur ») de Prodigy prétendait que la demanderesse était impliquée dans « une importante affaire de fraude ».

Dans une décision du 23 mai 1995, un juge de New York a considéré que le rôle de Prodigy était comparable à celui d'un éditeur (*publisher*) et non à celui d'un libraire ou distributeur (*distributor*). Conséquence : Prodigy pouvait être tenu pour responsable, alors qu'un distributeur ne peut l'être que s'il connaît ou a toutes les raisons de connaître le message diffamatoire. Plusieurs facteurs semblent avoir guidé la décision : l'image donnée par Prodigy dans sa publicité était celle d'un fournisseur de services pour les familles; la société laissait entendre qu'elle opérait un certain contrôle sur le contenu; Prodigy avait publié à l'attention des usagers des règles de conduite relatives aux contenus mis sur le réseau (afin d'éviter l'atteinte aux bonnes moeurs); la société utilisait un programme de tri permettant l'élimination des messages contenant des termes « incorrects »; un groupe d'experts avait été engagé de façon à assurer la mise en oeuvre des directives destinées aux usagers; ceux-ci disposaient d'un système permettant de détruire rapidement les messages suspects (Stratton Oakmont v. Prodigy Services Co., 1995 WL 323710, 23 Media L. Rep. 1794 (N. Y. Sup. Ct. 1995), *The Computer Law Association Bull.*, 1995, vol. 10, n° 4, p. 18-19).

352 Lire Y. BREBAN, « La responsabilité des acteurs de l'Internet », *Gaz. Pal* (Gazette du droit des technologies avancées), 25-26 octobre 1996, p. 23.

353 T. G. I. Paris (réf.), 12 juin 1996, *Expertises*, 1996, p. 277 et les obs. de A. Weber, « Droit de l'Internet. A la recherche des pierres angulaires », *Expertises*, 1996, pp. 274-275.

354 T. G. I. Paris (réf.), 23 mai 1996, Assoc. Relais et Châteaux c. Calvacom.

355 T. G. I. Paris (réf.), 16 avril 1996, Réf. 54240/96.

deur a fait valoir qu'aucun contrôle de l'accès et de la diffusion des informations sur le réseau ne pouvait être exercé, mais l'argument a été rejeté en des termes qui méritent d'être rapportés :

> « Attendu cependant que toute personne ayant pris la responsabilité de faire diffuser publiquement, par quelque mode de communication que ce soit, des propos mettant en cause la réputation d'un tiers doit être au moins en mesure, lorsque comme en l'espèce cette divulgation est constitutive d'un trouble manifestement illicite, de *justifier des efforts et démarches accomplis pour faire cesser l'atteinte aux droits d'autrui ou en limiter les effets* ».

Dans le cadre de l'action civile en réparation, le juge peut assouplir les conditions de la responsabilité — suivant en cela une nette tendance de la jurisprudence, discernable dans d'autres domaines[356] — de manière à faciliter l'indemnisation de la victime. Il peut notamment imposer des « standards objectifs de comportement », éventuellement élevés, dont la transgression est constitutive de faute : obligation de surveiller un site « suspect », obligation d'effectuer des contrôles aléatoires (par coups de sonde), obligation de justifier des actions entreprises pour supprimer des informations litigieuses, obligation de fermer l'accès à un site renseigné comme illicite, etc. Or, dans la mesure où les obligations mises à charge des FA se multiplient, les hypothèses où une faute, pratiquement objective, peut être stigmatisée deviennent aussi plus nombreuses. Autrement dit, il n'est pas exclu que l'on assiste, dans les années à venir, à une objectivation de la responsabilité, sous l'action de la jurisprudence.

IV.2.3. Les transporteurs

25. Les principes valent aussi, nous semble-t-il, pour les transporteurs qui, le plus souvent, se bornent à fournir des capacités de transmission et l'accès à un réseau de télécommunication[357]. Ils ne devraient pas être tenus d'une obligation de vérification systématique de l'information[358]. Mais leur responsabilité n'est pas exclue s'il peut être

356 Voy., par exemple, Y. LAMBERT-FAIVRE, « L'évolution de la responsabilité civile d'une dette de responsabilité à une créance d'indemnisation », *Rev. trim. dr. civ.*, 1987, p. 1-19; P. ESMEIN, « La faute et sa place dans la responsabilité civile », *Rev. trim. dr. civ.*, 1949, p. 481-490. Sur le fait que la multiplication des obligations de résultat entraîne un recul de la faute, voy. J. GHESTIN, « Les principes fondamentaux de la responsabilité à l'épreuve du droit communautaire », in N. FRASELLE (éd.), *La responsabilité du prestataire de services et du prestataire de soins de santé*, Bruxelles, Academia Bruylant, 1992, p. 28-41, spéc. p. 33.

357 Tel est certainement le cas des entreprises de télécommunication, qui ne peuvent avoir prise sur le contenu des messages transportés. Le statut des câblodistributeurs est, en revanche, plus ambigu, dans la mesure où il arrive qu'ils développent parfois des services dont ils assument une certaine maîtrise sur le contenu. A ce propos, voy. P. TRUDEL, « La protection des droits et des valeurs dans la gestion des réseaux ouverts », *op. cit.*, p. 27.

358 C'est ainsi, pour ne citer qu'un exemple, que le représentant de France Télécom a été relaxé dans une affaire où une messagerie télématique portait atteinte aux bonnes mœurs, au motif qu'il n'a pas été rapporté des éléments établissant que France Télécom avait connaissance de la violation par les fournisseurs de service de leur engagement et qu'étant un simple transporteur de messages, France Télécom ne pouvait pénétrer dans le système télématique pour contrôler tous les services ou les personnes qui les utilisent. Cf. T. G. I. Draguignan, 15 mai 1992, *D. I. T.*, 1991/4, p. 39-42.

établi qu'ils n'ont pris aucune mesure appropriée alors qu'ils savaient ou auraient dû savoir que des informations illicites circulaient sur les réseaux et qu'ils avaient les moyens d'empêcher cela. Au plan pénal, la responsabilité d'un transporteur, tout comme celle d'un FA ou d'un serveur, peut être recherchée sur le terrain de la complicité, lorsqu'il a sciemment, par aide ou assistance, facilité la consommation d'un crime ou d'un délit.

V. Réflexions finales

26. Un premier constat s'impose : le droit de la responsabilité est apte à prendre en charge les réseaux ouverts tel Internet. Certes, des difficultés se présentent, mais loin d'être toujours le propre d'Internet, elles tiennent plutôt, bien souvent, à la complexité ou aux lacunes du droit lui-même. Ce qui paraît certain, c'est qu'il n'y a pas de délit spécifique à Internet, mais des délits « de droit commun » commis sur Internet. Il n'y a pas lieu d'envisager, à la hâte, la création d'un droit spécial destiné à régir le réseau des réseaux, il « suffit » d'appliquer le(s) droit(s) existant(s). Cela ne veut pas dire qu'il ne faille l' (les) améliorer, çà et là, mais la question dépasse alors le cadre strict d'Internet.

Il est vrai que le caractère transnational du réseau, joint à la fugacité des contenus, n'est pas de nature à simplifier la tâche des juristes dans la détermination des règles applicables, dans l'administration de la preuve et dans la résolution des litiges. Et si la mondialisation ne doit pas constituer une excuse facile pour les législateurs nationaux, il reste que le risque existe de délocalisation des sites douteux vers des pays où les lois seraient moins contraignantes. D'où l'intérêt, souvent évoqué, d'une Convention internationale définissant des règles communes universellement applicables. Si celles-ci devaient porter sur les contenus, pareil souhait ne paraît ni réaliste ni souhaitable. Irréaliste car les valeurs et les sensibilités varient à ce point d'un pays à l'autre qu'il n'y aurait que deux façons de parvenir à un consensus : soit en restreignant à l'extrême le domaine des questions abordées, soit en limitant drastiquement le nombre de pays signataires. Non souhaitable, car nombre de valeurs devraient sans doute être sacrifiées sur l'autel du plus petit commun dénominateur. Dans les deux cas, l'exercice serait passablement inutile. Il serait bienvenu, par contre, pour la définition de principes communs sur des questions de forme, de procédure ou de méthode de solution des problèmes. Ainsi, il pourrait être envisagé d'adopter des principes communs concernant la détermination de la loi applicable, la coopération et l'entraide judiciaires et policières et, éventuellement, l'imputation des responsabilités[359].

Cela étant, il n'y a pas une solution unique au problème du contrôle des contenus sur Internet, mais des solutions complémentaires. Le législateur, les législateurs ont certes un rôle à jouer, mais il est aussi d'autres modes de régulation utiles voire nécessaires : les contrats conclus entre les

[359] Cf., en ce sens, la proposition française pour une charte de coopération internationale sur Internet, présentée à l'O. C. D. E. par le Ministre François Fillon, lors de la réunion qui s'est tenue à Séoul le 23 octobre 1996. Il est évident que l'adoption de principes communs sur le plan des procédures suppose un minimum de consensus sur le fond. Comme le suggère cette proposition, il s'agit de s'accorder sur certaines valeurs, formulées, il est vrai, en des termes très généraux : respect de l'ordre public, protection de la vie privée, des consommateurs, des droits d'auteur...

acteurs, les codes de déontologie élaborés par les professionnels de l'Internet, des solutions techniques telles que, le cas échéant, des dispositifs de filtrage à usage des familles...

VI. Bibliographie sélective

A. U. I. , « Pour une intégration sereine et un développement harmonieux d'Internet dans la société française », Rapport du 7 juin 1996, disponible sur le site de l'A.U.I. (http://www.aui.fr).

A. U. I. , « Amendement Fillon sur le contrôle d'Internet : précipité, inutile, injustifié, techniquement inapplicable et dangereux pour la démocratie et la liberté », disponible sur le site de l'A.U.I. (http://www.aui.fr).

M. BEEREPOOT, « Liability of access and service providers for online content », 6 p.

(<http://www.iway.fr/groupecx/uae/Comptes-rendus.html>).

H. BITAN, « L'Internet représente-t-il une menace pour l'ordre public ? », *Expertises*, 1996, p. 266-270.

Y. BREBAN, « La responsabilité des acteurs de l'Internet », *Gaz.Pal.* (Gazette du droit des technologies avancées), 25-26 octobre 1996, pp. 21-24.

J. -P. BUYLE, O. POELMANS, « Internet : quelques aspects juridiques », *D.I.T.*, 1996/2 (première partie), pp. 10-18.

D. CALOW, « Defamation on the Internet », *C.L.S.R.* , 1995, pp. 199-200.

I. FALQUE-PIERROTIN (sous la présidence de), *Rapport de la Mission Interministérielle sur l'Internet*, 16 juin 1996. Une synthèse de ce rapport est disponible sur Internet à l'adresse suivante : http://www.telecom.gouv.fr./français/activ/techno/missionint.htm

N. GAUTRAUD, « Internet, le législateur et le juge », *Gaz.Pal.* (Gazette du droit des technologies avancées), 25-26 octobre 1996, pp. 60-65.

C. HENNAU, J. VERHAEGEN, *Droit pénal général*, 2e éd. revue et mise à jour, Travaux de la Faculté de Droit de l'U.C.L., Bruxelles, Bruylant, 1995.

G. HUGHES, D. COSGRAVE, « Legal questions involving the Internet », *C.L.S.R.*, 1995, pp. 321-324.

H. W. K. , KASPERSEN, « Aansprakelijkheid van Internet-providers », *Computerr.*, 1996/2, pp. 9-13.

Q. KROES, « Internet, aansprakelijkheid in het Amerikaanse recht », *Computerr.*, 1996/1, pp. 5-9.

J. -J. LAVENUE, « Cyberespace et droit international : pour un nouveau jus communicationis », *R.R.J.*, 1996-3, pp. 811-844.

F. OLIVIER, E. BARBRY, « Des réseaux aux autoroutes de l'information : révolution technique ? Révolution juridique ? 2. Du contenu informationnel sur les réseaux », *J.C.P.*, G, 1996, I, 3928, p. 179-186.

F. RIGAUX, M. FALLON, *Droit international privé*, t. II, 2e éd. refondue, Précis de la Faculté de Droit de l'U.C.L., Bruxelles, Larcier, 1993.

N. RISACHER, « Internet et la protection des droits fondamentaux de la personne humaine », *Lamy droit de l'informatique*, N° 82, C, 1996, p. 1-4.

A. TAEBI, « Self regulation on the Internet », *C. L. S. R.* , 1995, pp. 202-203.

P. TRUDEL, « La protection des droits et des valeurs dans la gestion des réseaux ouverts », disponible sur Internet (http://www.droit.umontreal.ca/CRDP/).

P. TRUDEL, « Introduction au droit du commerce électronique sur l'Internet », *Revue du Barreau*, 1995, vol. 55, pp. 521-551.

F. TULKENS, M. VAN DE KERCHOVE, *Introduction au droit pénal*, 2e éd. revue et mise à jour, A la rencontre du droit, Bruxelles, E. Story-scientia, 1993.

M. VIVANT, « Cybermonde : Droit et droits des réseaux », *J.C.P.*, G, 1996, I, 3969, pp. 401-407.

A. WEBER, « Droit de l'Internet. A la recherche des pierres angulaires », *Expertises*, 1996, pp. 274-275.